7Ш

УДК 681.31

Б.М. Шевчук
Інститут кібернетики ім. В.М. Глушкова НАН України, м. Київ
Україна, 03680 МСП, м. Київ, проспект Академіка Глушкова, 40, *incors@ukr.net*

Прихована та захищена передача інформації в сенсорних і локально-регіональних радіомережах

B.M. Shevchuk
Glushkov Institute of Cybernetics of National Academy of Sciences of Ukraine, c. Kyiv
Ukraine, 03680 MSP, c. Kyiv, Glushkova ave., 40 , incors@ukr.net

Hidden and Protected Data Transfer in Sensor and Local-Regional Radio Networks

Б.М. Шевчук
Институт кибернетики им. В.М. Глушкова НАН Украины
Украина, 03680 МСП, проспект Академика Глушкова, 40, *incors@ukr.net*

Скрытая и защищенная передача информации в сенсорных и локально-региональных радиосетях

Для реалізації прихованої у шумах радіоканалу та захищеної передачі пакетів даних у радіомережах на кожній абонентській системі запропонована реалізація комплексу алгоритмів, включаючи компактне кодування даних, криптостійке кодування даних з використанням одноразових шифрів, завадостійке кодування даних пакетів з використанням абонентом-відправником та абонентом-отримувачем пакету генерації псевдовипадкових послідовностей, перемішування даних та формування шумоподібних інтервально-імпульсних послідовностей з базою сигналу, яка попередньо узгоджена з поточним рівнем шумів у каналі зв’язку.

Ключові слова: прихована та захищена передача інформації, крипостійке та завадостійке кодування, шумоподібні інтервально-імпульсні послідовності, база сигналу.

To implement in radio networks secure data transfer hidden in radio noises on each subscriber system, it is proposed the implementation of complex algorithms and crypto-resistant encoding data with single-use codes, antinoise encoding data packets with a subscriber-sender and recipient of the call-receiver package generation pseudorandom sequences, data mixing and formation of noise-interval pulse sequence with a base signal that previously coordinated with the current noise in the channel of communication.

Key words: hidden and secure data transfer, crypto-resistant and antinoise coding, noise-like interval-pulse sequence, base for signal.

Для реализации скрытой в шумах радиоканала и защищенной передачи пакетов данных в радиосетях на на каждой абонентской системе предложена реализация комплекса алгоритмов, включая компактное кодирование данных, криптоустойчивое кодирование данных с использованием одноразовых шифров, помехоустойчивое кодирование данных пакетов с использованием абонентом-отправителем и абонентом-получателем пакета генерации псевдослучайных последовательностей, перемешивание данных и формирование шумоподобных интервально-импульсных последовательностей с базой сигнала, которая предварительно согласована с текущим уровнем шумов в канале связи.

Ключевые слова: скрытая и защищенная передача информации, криптоустойчивое и помехоустойчивое кодирование, шумоподобные интервально-импульсные последствия, база сигнала.

Вступ

З розвитком інформаційно-комунікаційних технологій широкого використання в різних галузях людської діяльності отримали сенсорні мережі (СМ). Програмно-апаратні засоби СМ є основою для побудови бортових систем мобільних роботів, безпілотних апаратів, портативних пристроїв контрольованих осіб, стаціонарних об'-єктів моніторингу. У режимі тривалого спостереження за станом об'єктів (промислових, сільськогосподарських, охоронних, об'єктів екомоніторингу, телемедицини, рухомих об'єктів, та ін.) автономні засоби СМ забезпечують введення, оброблення, накопичення та передавання даних моніторингу на центральний сервер СМ. При цьому автономні засоби СМ, до яких відносяться повнофункціональні пристрої (абонентські (АС) і об'єктні системи (ОС)), пристрої з обмеженими функціями, роутери (абонентські системи-ретранслятори), об'єднуються в комірки, кластери комірок та тривало працюють в режимі очікування і накопичення первинних даних, а також виявляють найбільш інформативні дані і передають їх в дистанційні локальні та центральні бази даних. Моніторинговими даними можуть бути масиви вимірювальних сигналів, дискретних повідомлень, ключові кадри відеоданих, стислі та закодовані масиви даних.

Шляхом розгортання сенсорних і локально-регіональних радіомереж у вигляді комірок та кластерів комірок на заданій території в режимі самоорганізації передачі пакетів інформації забезпечується ретрансляція моніторингових даних на великі відстані. В [1-3] запропоновані методи та алгоритми реалізації ефективних за швидкодією і точністю компактного та криптостійкого кодування сигналів і відеосигналів для побудови інформаційно-ефективних АС (ОС) сенсорних мереж.

Невирішеною проблемою побудови засобів СМ є забезпечення захищеної (криптостійкої та завадостійкої) передачі інформаційних пакетів (ІП) в умовах дії та проникнення в радіоканал системних завад, які виникають від роботи сусідніх абонентських станцій радіомереж, імпульсних вузькосмугових та широкосмугових завад, створених несанкціонованими абонентами СМ та в процесі роботи промислового обладнання, електротранспорту та ін.

Постановка задачі. Враховуючи малу потужність радіопередавачів модулів ISM-діапазону частот (ISM-industrial, scientific, medical 433 МГц, 868 МГц, 902-928 МГц (для США), 2.4 ГГц)) , які є радіотехнічною основою для побудови АС (ОС) сенсорних мереж, актуальною проблемою при застосуванні СМ є реалізація надійної та захищеної передачі інформації між віддаленими абонентами мережі. Дані проблеми вирішуються комплексно, на радіотехнічному та інформаційному рівнях обробки і передачі інформації, а саме: за рахунок підвищення ефективності радіотехнічних засобів (шляхом використання направлених антен, інтелектуальних мініатюрних антенних систем з формуванням та підтримкою направлених діаграм випромінювання високочастотних сигналів в сторону абонента-отримувача ІП); шляхом формування в процесі передачі пакетів відповідних сигнально-кодових послідовностей. З урахуванням використання потужних об'єктних процесорів та спеціалізованих пристроїв цифрової обробки даних (ARM7-11, мікропотужних сигнальних процесорів, ПЛІС) доцільно на інформаційному рівні формувати компактні, криптостійкі та завадостійкі ІП.

Метою даної статті є розробка методології ефективної передачі в СМ ІП, прихованих у шумах радіоканалу та захищених від дій потужних імпульсних завад та несанкціонованих користувачів СМ. При цьому основою прихованої та надійної передачі ІП в шумах радіоканалу є реалізація парою абонентів «відправник – отримувач ІП» відомих тільки їм методів кодування первинних даних та формування шумоподібних інтервально-імпульсних сигналів, адаптованих до рівня шумів у каналі зв'язку.

Реалізація прихованої та захищеної передачі пакетів інформації в сенсорних радіомережах

Прихована передача інформації у шумах радіоканалу передбачає в процесі передачі ІП формування сигнально-кодових конструкцій, параметри яких максимально наближені до характеристик флуктуаційних завад природного походження, за модель яких, як правило, приймають білий гаусівський шум, що має рівномірний спектр. Відомі різноманітні типи прихованої передачі інформації, включаючи енергетичну, структурну, інформаційну [4-6]. У СМ широкого застосування найбільш доцільна реалізація на інформаційному рівні формування сигнально-кодових послідовностей, передача і прийом яких здійснюється в шумах радіоканалу. По суті мова йде про те, щоб, незважаючи на рівень шумів в радіоканалі та ймовірність доступу до нього несанкціонованих користувачів мережі, з використанням стандартних і недорогих радіотехнічних засобів, організувати надійну та захищену передачу інформації між парою абонентів «відправник – отримувач ІП». Саме пари абонентів, з урахуванням прийнятих за основу ступенів захисту даних в СМ, забезпечують надійну та захищену передачу ІП. Усі інші системні заходи захисту даних в СМ та в мережах вищого рівня додатково забезпечують умови реалізації надійної і захищеної передачі конфіденційних даних. Основою прихованої передачі інформації в шумах радіоканалу є підтримка парами абонентів мінімально необхідного енергетичного співвідношення сигнал/шум в радіоканалі $(E_b / J_o)_n$ [4], де $E_b = P_c \cdot T_b$ – енергія сигналу, яка припадає на інформаційний символ (питома енергія інформаційного символу), P_c – потужність сигналу, T_b – тривалість інформаційного символу, $J_o = J / F$, J – середня потужність сумарних завад у каналі зв'язку (в точці прийому інформації), F – робоча смуга частот радіоканалу. Ефективним способом прихованої передачі цифрових даних є формування інтервально-імпульсних послідовностей [3], які передаються шумоподібними сигналами (ШПС) із заданою базою і структурою. У результаті відповідні інформаційні символи (двійкові послідовності) передаються шумоподібними сигнально-кодовими послідовностями певної тривалості, параметри яких узгоджені з поточним рівнем шумів у каналі зв'язку. Слід зазначити, що очікуваний ефект від використання ШПС можливий при виборі бази ШПС $B > 10\log_2 n$ [4,6], де $B = F \cdot T = F / R$, $T = T_b$ – тривалість ШПС, n – основа алфавіту джерела інформації ($n = 2$), R – швидкість передачі інформації. При цьому в процесі встановлення зв'язку або при перевірці якості каналу зв'язку (оцінки поточного співвідношення сигнал/шум в радіоканалі) абонент «відправник ІП» передає абоненту «отримувачу ІП» тестовий пакет. На основі аналізу якості прийому інтервальних послідовностей, заповнених ШПС з різними за величиною базами, відповідною парою абонентів приймається рішення про передачу поточного ІП з мінімально необхідною базою, при якій забезпечується необхідне енергетичне співвідношення сигнал/шум у радіоканалі. У результаті сформовані сигнально-кодові послідовності будуть замасковані в шумах радіоканалу. Ті інформаційні символи, які будуть вражені шумами, відновлюються методами завадостійкого кодування даних.

При обмеженій смузі частот F характеристики системи передачі інформації з ШПС, такі, як швидкість і завадостійкість передачі даних, кількість одночасно працюючих пар абонентів у спільному радіоканалі (кількість незалежних моно- каналів L у спільній робочій смузі радіочастот) є взаємозалежними величинами і можуть бути визначені зі співвідношень [6], [7]

$$h^2 = B \cdot h_0^2,\ L \le B / 4,$$

де h^2 – відношення сигнал/шум на виході приймача ШПС, h_0^2 – відношення сигнал/шум на вході приймача ШПС.

Якість маскування передачі інформації в шумах радіоканалу можливо оцінити по вихідному сигналу кореляційного обчислювача в точці прийому шумоподібного ІП. Для оперативної кореляційної обробки вихідних сигналів демодулятора радіоприймача об'єктної системи доцільно реалізувати обчислювач взаємомодульної функції, яка визначається виразом:

$$G(j) = \sum_{i=1}^{B} \left| S_i - X_{i+j} \right|,$$

де $G(j)$ – відліки модульної функції при j-му зсуві відліків вхідного сигналу X_i, $j = 0,1,2,..., B,...,2B,...$ – значення часового зсуву, S_i – i-й елемент опорного ШПС.

Дослідження поведінки функції $G(j)$ при різних рівнях шумів в каналі зв'язку показали, що величина бази ШПС розподіляється на складові:

$$B = L + П_ш + M + H,$$

де $П_ш \approx 0.5B$ – поріг розпізнавання сигналу від шуму, M – оцінка ступеня «зашумленості» каналу зв'язку, в якому забезпечується достовірний прийом інформації, $H > 1$ – величина, яка характеризує якість прийому інформаційного символу.

Умовою маскування інформації в шумах каналу зв'язку та достовірного прийому поточного інформаційного символу є виконання умови $G(j) \to B/2$ на відповідному елементарному інтервалі ШПС, місцезнаходження якого відоме тільки двом абонентам, що здійснюють передачу і прийом ІП. На рис.1. наведений приклад вихідного сигналу корелятора в процесі прийому шумоподібного інформаційного символу, прихованого в шумах радіоканалу.

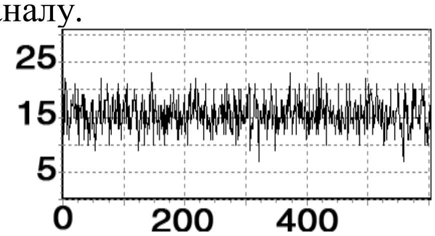


Рисунок 1 – Вихідний сигнал кореляційного приймача, отриманого при прийомі шумоподібного ІП, прихованого в шумах радіоканалу

Ефективне вирішення проблеми передачі даних в сенсорних та локально-регіональних радіомережах досягається шляхом реалізації засобами об'єктних систем комплексу методів і алгоритмів компактного кодування сигналів (відеосигналів), оперативного стиску-захисту масивів даних [1-3], завадостійкого кодування даних з використання кодів Галуа [8], перемішування даних. У процесі формування і передачі інервально-імпульсних послідовностей ІП можна використати різні типи ШПС та ефективні методи передачі і прийому даних з ШПС [5], [7-10]. Для криптографічного захисту даних ІП доцільно використовувати прості операції сумування по модулю два компактних масивів даних та згенерованих псевдовипадкових послідовностей. При цьому ключі шифрування даних повинні змінюватись від пакету до пакету, для чого кожна ОС мережі повинна володіти закритим і відкритим ключем, на основі яких реалізуються процедури шифрування/дешифрування ІП.

Реальну швидкість передачі даних з використанням ШПС в радіомережах можна визначити виразом

$$R = K_c \cdot L / k_s \cdot T_b \cdot B,$$

де $K_c = K_i \cdot K_{rt}$ – сумарний коефіцієнт стиску даних, K_i – коефіцієнт стиску даних на інформаційному рівні (враховує стиск даних з допустимими втратами інфор-

мації та стиск даних без втрат), K_{rt} – коефіцієнт стиску даних на радіотехнічному рівні (враховує підвищення швидкості передачі даних за рахунок багатопозиційних методів маніпуляції даних), $k_s > 1{,}4 - 1{,}8$ – коефіцієнт, що враховує якість відновлення фронтів цифрових сигналів [4].

З урахуванням використання спрощених радіотехнічних засобів, що характерно для ОС сенсорних мереж, ефективність прихованої і захищеної передачі інформації можливо підвищити за рахунок оптимізації величини $K_c \to \max K_c$, де $K_c = k_1 \cdot k_2 \cdot k_3 \cdot k_4$, k_1 – коефіцієнт стиску даних з допустимими втратами інформації (визначається особливостями прикладних досліджень і завдань), k_2 – коефіцієнт стиску без втрат ($k_{2\min} \approx 1.4 - 2$), k_3 – коефіцієнт ущільнення даних у процесі реалізації завадостійкого кодування ($k_{3\min} \approx 1{,}4$), k_4 – коефіцієнт ущільнення даних у процесі формування інтервально-імпульсних послідовностей ($k_4 \geq 1.4 - 2$). Таким чином, за рахунок оперативної реалізації комплексу взаємодоповнюючих методів і алгоритмів компактного, криптостійкого та завадостійкого кодування даних засобами ОС в канал зв'язку передаються беззбиткові компактні та захищені дані. При цьому захист даних від спотворення канальними завадами є багаторівневим, що дозволяє мінімізувати повторну передачу і ретрансляцію пакетів.

Висновки

Ефективна реалізація прихованої та захищеної передачі інформації в сенсорних та локально-регіональних радіомережах досягається за рахунок побудови інформаційно-ефективних об'єктних систем, процесорні засоби яких у місцях введення даних (вимірювальних сигналів, зображень, масивів даних) забезпечують виконання комплексу взаємодоповнюючих методів і алгоритмів компактного кодування даних, криптостійкого та завадостійкого кодування даних ІП, формування шумоподібних інтервально-імпульсних сигналів з базою, яка забезпечує мінімально необхідне енергетичне співвідношення сигнал/шум в каналі зв'язку. Передача даних здійснюється на рівні шумів радіоканалу, і для її прийому необхідно володіти поточними секретними ключами, які є тільки у абонента «відправника ІП» та абонента «отримувача ІП».

Стаття написана і опублікована за підтримки Державного фонду фундаментальних досліджень України, проект № Ф41.2/028 «Розробка та дослідження методів і алгоритмів прихованої та захищеної передачі інформації в задачах групового управління мобільними роботами і рухомими системами».

Література

1. Шевчук Б.М. Оперативне формування і передавання компактних, криптостійких та завадостійких пакетів інформації в радіомережах // Комп'ютерні засоби, мережі та системи. – 2011. – № 10. – С. 143-152.
2. Шевчук Б.М. Підвищення ефективності передачі пакетів інформації в сенсорних та локально-регіональних радіомережах для організації зв'язку між мобільними роботами і рухомими системами // Штучний інтелект. – 2011. – № 3. – С. 417-422.
3. Шевчук Б.М. Технологія багатофункціональної обробки і передачі інформації в моніторингових мережах / [Шевчук Б.М., Задірака В.К., Гнатів Л.О., Фраєр С.В.]. – К. : Наук. думка, 2010. – 370 с.
4. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Скляр Б. – [2-е изд., пер. с англ.]. – М. : Издательский дом «Вильямс», 2003. – 1104 с.
5. Голубничий О.Г. Методи забезпечення прихованості передавання інформації у широкосмугових радіосистемах: автореф. дис. на здобуття наук. ступеня канд. техн. наук / Голубничий О.Г. – К., 2010. – 20 с.

6. Варакин Л.Е. Системы связи с шумоподобными сигналами / Варакин Л.Е. – М. : Радио и связь, 1985. – 384 с.
7. Голяницкий И.А. Математические модели и методы в радиосвязи / Голяницкий И.А. ; под ред. Ю.А. Громакова. – М. : Экотрендз, 2005. – 440 с.
8. Патент України № 96853, Н03М 13/00. Спосіб передавання та приймання інформації / Николайчук Я.М., Гринчишин Т.М., Воронич А.Р. – 2011. – Бюл. № 23. – 6 с.
9. Урядников Ю.Ф. Сверхширокополосная связь. Теория и применение / Ю.Ф. Урядников, С.С. Аджемов. – М. : СОЛОН-Пресс, 20005. – 368 с.
10. Николайчук Я.М. Інформаційні міри ентропії та їх застосування в комп'ютерних системах і мережах / Я.М. Николайчук, А.Р. Воронич, І.О. Погонець // Матеріали проблемно-наукової міжгалузевої конф. «Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки та моделювання» (ПНМК-2012). – Бучач : Бучацький інститут менеджменту і аудиту. – 2012. – Вип. 8. – С. 136-140.

Literatura

1. Shevchuk B.M. Komp'juterni zasoby, merezhi ta systemy. 2011. № 10. S. 143-152.
2. Shevchuk B.M. Shtuchnij intelekt. 2011. № 3. S. 417-422.
3. Shevchuk B.M. Tehnologija bagatofunkcional'noi obrobky i peredachi informacii v monitoryngovyh merezhah. K.: Nauk. Dumka. 2010. 370s.
4. Skljar B. Cifrovaja svjaz'. Teoreticheskie osnovy i prakticheskoe primenenie. M.: Izdatel'skij dom "Vil'jams". 2003. 1104 s.
5. Golubnychij O.G. Metody zabezpechennja pryhovanosti peredavannja informacii u shyrokosmugovyh radiosystemah. Avtoref. na zdobuttja naukovogo stupenja kandydata tehnichnyh nauk. K.: 2010. 20 s.
6. Varakin L.E. Sistemy svjazi s shumopodobnymi signalami. M.: Radio i svjaz'. 1985. 384 s.
7. Goljanickij I.A. Matematicheskie modeli i metody v radiosvjazi. Pod red. Ju.A. Gromakova. M.: Jekotrendz. 2005. 440 s.
8. Nikolajchuk Ja.M., Grinchishin T.M., Voronich A.R. Sposib peredavannja ta pryjmannja informacii. Patent Ukrainy № 96853, H03M 13/00. – Bjul. №23, 2011. – 6 s.
9. Urjadnikov Ju.F. Sverhshirokopolosnaja svja'. Teorija i primenenie. M.: SOLON-Press. 2005. 368 s
10. Nikolajchuk Ja.M. Materialy problemno-naukovoi mizhgaluzevoi konf. "Informacijni problemy komp'juternyh system, jurysprudencii, energetyky, ekonomiky ta modeljuvannja" (PNMK-2012). Buchach: Buchachs'kyj instytut menedzhmentu i audytu. 2012. Vyp. 8. S. 136-140.

RESUME

B.M. Shevchuk

Hidden and Protected Data Transfer in Sensor and Local-Regional Radio Networks

To implement in radio networks secure data transfer hidden in radio noises on each subscriber system, it is proposed the implementation of complex algorithms and crypto-resistant encoding data with single-use codes, antinoise encoding data packets with a subscriber-sender and recipient of the call-receiver package generation pseudorandom sequences, data mixing and formation of noise-interval pulse sequence with a base signal that previously coordinated with the current noise in the channel of communication. As a result of complex coding for each subscriber radio system, compact and protected (crypto-resistant and noise stability) packets of information are sent to the radio channel.

Compact coding reduces the number of transmitted packets of information, crypto-resistant coding provides data protection against distortion and access to unauthorized users of radio, antinoise coding ensures rapid recovery of single and group errors arising from the noise of the channel, the mixing of data prevents the emergence of long distorted bit sequence and the use of noise-like signals with minimal signal of necessary framework provides the necessary energy in the communication channel and hides message digit in the channel noises.

Стаття надійшла до редакції 02. 07.2012.